ABSTRACT OF THE DISCLOSURE

In order to verify the authenticity of manufactured goods, a smart tag is attached to the goods containing encrypted authentication information, such as a serial number, a description of the good's physical appearance or chemical decomposition, its color, or digital images of the good etc. The encryption procedure comprises public/private key encryption with zero-knowledge protocols. Zero knowledge protocols allow a smart tag to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without revealing its authentication information. The verification procedure can be done using a reader at a point of sale (POS) machine equipped with the appropriate public key and zero-knowledge protocols to decrypt the authentication information. A printed version of the serial number or other authentication information may be placed on the goods in human readable form to quickly verify the information electronically read from the smart tag. With the present invention, only the manufacturer can create such smart tags with the associated data thus making it virtually impossible to pass off a counterfeit good as authentic. In addition to authenticating counterfeit goods, the present invention can be used to detect authentic goods being sold in a parallel market.